

# GALOIS FIELD MULTIPLY ACCUMULATOR

Andrew J. Thurston

## ABSTRACT OF THE DISCLOSURE

An OC-192 front-end application-specific integrated circuit (ASIC) de-  
5 interleaves an OC-192 signal to create four OC-48 signals, and decodes error-  
correction codes embedded in each of the four OC-48 signals. The decoder generates  
a Bose-Chaudhuri-Hocquenghem (BCH) error polynomial in no more than 12 clock  
cycles. The decoder includes several Galois field multiply accumulators, and a state  
machine which controls the Galois field units. In the specific embodiment wherein  
10 the error-correction code is a BCH triple error-correcting code, four Galois field units  
are used to carry out only six equations to solve the error polynomial. The Galois  
field units are advantageously designed to complete a Galois field  
multiply/accumulate operation in a single clock cycle. The Galois field units may  
operate in multiply or addition pass-through modes. An error insertion circuit is also  
15 provided for verifying correct operation of the BCH encoding and decoding circuits.  
A desired number of errors may be programmed for insertion into the OC-48 data  
signals. Error insertion may be performed in an iterative fashion to insert into  
different data signals the desired number of errors, wherein the errors are placed  
within the code words of the data signals at different location permutations for each  
20 data signal. In one implementation, error verification is performed using an error  
accumulator located in the receiver, and means are provided for examining an error  
accumulator count of the error accumulator to see if the number of accumulated errors  
matches with the number of inserted errors.